REMARKS

This is in full and timely response to the above-identified Office Action. The above listing of the claims supersedes any previous listing. Favorable reexamination and reconsideration is respectfully requested in view of the preceding amendments and the following remarks.

Rejections under 35 USC § 112

In this response minor amendments to the claims have been proposed to improve syntax and form. These amendments neither affect the scope of the claims nor raise any question as to whether a further search or consideration is necessary.

The Applicant, however, traverses the position taken by the Examiner that the use of the term "substantially" renders the claims indefinite. Indeed, the removal of this term could be seen as having a marked effect on the scope of the claim from which it is removed. The Examiner's attention is called to the fact that the use of the term "substantially" in the context that it used, actually emphasizes the difference rather than diluting the same. That is to say, just any difference and a substantial difference are seen as being substantially different. Indeed, it is not seen that the use of this term requires a standard for ascertaining the "requisite degree" or that one of ordinary skill in the art would fail to be reasonably appraised of the scope of the invention due to the use of this term.

It is also noted that, on page 4 of this Office Action, the Examiner has stated that "Spies does not specifically disclose an index further comprising credential information differing substantially from the credential such that the credential is not disclosed by the index." (Emphasis added) It is submitted that, at least for the sake of rejection, the term "substantially" has not presented any lack of clarity.

Favorable reconsideration is respectfully requested.

Rejections under 35 USC § 103

The rejection of claims 1-21 under 35 USC § 103(a) as being unpatentable over Spies et al. (U.S. Patent 5,689,565) in view of Schiedt et al. (U.S. Patent 6,754,820), is traversed.

In a nutshell, the Spies reference discloses the idea that cryptographic operations are

supplied to a local application by means of a driver architecture. An application calls a standard interface, which selects a specific service provider (a.k.a. library) to perform the cryptographic operation. This is all local to the machine. As part of the initialization the service provides supply a set of services that they offer.

The scheidt et al. reference discloses an object (e.g. a word document) needs to be protected so that only particular individuals can access it. (Role based Access Control). The mechanism used to achieve this is such as to encrypt the document with a random key. This random key is then encrypted in multiple ways so that each of the potential assessors can decrypt it in the specific way.

In comparison, the claimed arrangement is such that a list of credential types that one is prepared to disclose, is sent. The recipient selects which credential types are such as to provide an acceptable assurance. This selection is sent back to the user and the user reveals the chosen credentials.

The Spies reference uses the advertising of the services provided by each of the installed cryptographic modules. The CAPI interface chooses the appropriate module to perform the desired cryptographic operation. The modules reveal a set of services they offer - rather than a set of credentials they are prepared to reveal - *ego* no credential index is sent or reviewed for selection purposes.

The Scheidt et al. reference sets forth an arrangement wherein the only certain parties are permitted to access an object. The object is "in full view of everyone" however not everyone can decrypt. In the claimed arrangement, the credentials are supplied to only those who ask for them and there is no notion of withholding information - merely streamlining the choosing of acceptable credentials.

The Spies/Scheidt arrangements use the idea that installed software registers its capability. This is then used to choose a software module when a specific cryptographic capability is required. A distinct difference with the claimed subject matter is that the claimed arrangement is open ended. The fact that all of the credentials can be understood is not important, just if there are some credentials that are understood and accepted.

In this Office Action the Examiner has taken the position that Spies discloses a credential index by "showing level of user profiles for the purpose of validating user's access to date

information." Indeed on page 13 of this Office Action, the Examiner has taken the pains to specify that Spies discloses "the cld is the credential index, d.sub.c is the category, x.sub.c is the private key for the credential, y.sub.c is the public key for the credential, and .lambda..sub.c is the MLA level defined for the credential by the domain authority. " Column 7, line 14 to column 8, line 63 and column 10 lines 10-65 are cited as supporting this position.

However, a review of the cited sections of the Spies reference reveals a total dearth of this disclosure. In fact, an electronic review of the whole Spies reference reveals that there is no ".sub.c" disclosed anywhere in the document, let alone the values quoted as refuting the Applicant's position that Spies does not in fact disclose a "credential index."

It is therefore submitted that the very foundation for the Examiner's position is evidenced as missing along with any support for a tenable argument that could cogently refute the Applicant's position that Spies does not disclose a "credential index." It is therefore submitted that the rejection almost seems based on a different reference and clearly fails to establish a *prima facie* case of obviousness for at least this reason.

> To establish *prima facie* obviousness of a claimed invention, all the claim limitations **must be taught or suggested** by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). M.P.E.P. § 2143.03. Accord M.P.E.P. § 706.02(j). (Emphasis added)

Further, in order to establish a *prima facie* case of obviousness, it is necessary to show that the hypothetical person of ordinary skill would, without any knowledge of the claimed subject matter and without any inventive activity, be motivated to arrive at the claimed subject matter given the guidance of the cited references when each is fully considered as statutorily required.

Indeed, if this rejection is to be maintained, proper foundation for the position that that the Spies reference teaches the use of a "credential index", in a manner that the hypothetical person of ordinary skill would be lead to understand its existence, must be established by at least pointing out where the purportedly disclosed values are set forth and how these values would lead the hypothetical person of ordinary skill to the position assumed in this rejection.

Further, even if (arguendo) the disclosure of a "credential index" *per se* could be shown to exist in the Spies reference, the need exits to demonstrate the claimed interaction actually takes

place between the various parties involved, actually. For example, in connection with the requirement in claim 1, for "a user causing a sender to communicate to a recipient a credential index", all that is cited is the sender is "participant 22a fig, 1" and the recipient is "participant 22b fig. 1." At best, all that the rejection is established is that communication between 22a and 22b is possible. The "causing" step remains unidentified. Indeed, a careful review of Figs, 1 and 2, the abstract; column 5, line 21 – column 6, line 24, and column 6, lines 36 – column 7, line 28, and column 10, lines 10-65, fails to reveal any disclose in Spies of the what the Office Action purports to be disclosed.

For example, the abstract discloses:

> A cryptography system architecture provides cryptographic functionality to support an application requiring encryption, decryption, signing, and verification of electronic messages. The cryptography system has a cryptographic application program interface (CAPI) which interfaces with the application to receive requests for cryptographic functions. The cryptographic system further includes at least one cryptography service provider (CSP) that is independent from, but dynamically accessible by, the CAPI. The CSP provides the cryptographic functionality and manages the secret cryptographic keys. In particular, the CSP prevents exposure of the encryption keys in a non-encrypted form to the CAPI or application. The cryptographic system also has a private application program interface (PAPI) to provide direct access between the CSP and the user. The PAPI enables the user to confirm or reject certain requested cryptographic functions, such as digitally signing the messages or exportation of keys.

The Applicant therefore questions as to the pertinence of at least this disclosure with respect to the position taken in this Office Action.

The arrangement Spies discloses is such that each of the participants registers a packet of information with an independent third party (i.e. the credential binding server 26 in Figs. 1 and 2) - see the registration process described at column 8, line 12 - column 11, line 20. This credential binding server 26 then performs a two step verification process - see column 10, lines 48-60:

> The credential binding server 28 then performs a two-step verification technique to verify that the packet actually originated from the participant, and not an impostor. At step 96, the **credential binding server 28 recalculates the participant's digital signature** by **hashing** the data contained in the decrypted registration packet using the same hashing function employed by the participant. The **recalculated hash is then compared with the decrypted hash received as a digital signature**, i.e., privately encrypted hash, in the registration packet (step 98 in FIG. 5). If the two hashes match, the credential binding server is assured both that the registration packet was indeed signed by the participant and that the contents have not been subsequently altered. (Emphasis added)

However, at no time does the Spies arrangement cause a "recipient" to respond to an index communicated by a "sender" by (a) responding to an indication of a selected at least one credential communicated by the recipient by selecting at least one of the credentials from the index of at least one credential provided by the sender, and (b) communicating to the sender an indication of the selected at least one credential. This simply does not happen and there is no disclosure which even remotely suggests the same.

Indeed, if this rejection is to be maintained the Examiner must also establish without question that the Spies reference is such that one of the parties involved selects one credential from the index and requests the other party to provide the credential corresponding to that which is selected from the index. Thus, the Examiner must show that the "recipient" responds to the index communicated by the "sender" by (a) responding to an indication of a selected at least one credential communicated by the recipient by selecting at least one of the credentials from the index provided by the sender, and (b) communicating this selection to the "sender", and then having the "sender" provide to the "recipient" at least one credential corresponding to the selected at least one credential.

The rejection of all the pending claims suffers from this fatal shortcoming. The rejection cannot be properly maintained irrespective of the citation of Scheidt et al. Indeed, the teachings of Scheidt et al. merely serve to muddy the waters.

The Office Action admits Spies does not disclose an index further comprising credential information differing "substantially" from the credential such that the credential is not disclosed by the index. Because Spies does not disclose the index as claimed, any consideration of the proposed modification of this non-disclosed/suggested index with the Scheidt et al. disclosure would seem to be mooted.

The index Spies discloses indicates the strongest algorithm and key size and is placed on each participant's credential; see column 15, lines 25-27.

While Scheidt et al. mentions a credential index there is no expectation that the hypothetical person of ordinary skill would be inclined to consider a transfer from a reference which explicitly mentions a credential index to Spies which, at best, fails to disclose its existence to the degree that it cannot even be inferred as existing, merely for the sake of having a feature which is set forth in the claims, must be deemed dubious at best. At the very least, it is clear from the rejection that the hypothetical person of ordinary skill would need to known that it was appropriate to select "secret" from the plurality of disclosed security levels/categories in order to make any use of the teachings of Scheidt et al. Just what teachings in either of the references relied upon for rejection, can be advanced to lead the hypothetical person of ordinary skill to this conclusion, is not at all clear, and in fact is submitted as being non-existent.

A further flaw in this rejection is found in the position taken by the Examiner in connection with the position taken that the "applicant has recognized another advantage which would flow naturally from following the suggestion of the prior art" and that this "cannot be the basis for patentability when the difference would otherwise be obvious." There is no foundation for this position, nor the position that the motivation for combination "would have provided sensitivity level or multiple level access control such that the access to credentials depending on the method of member identification and enforced domain authority dictated policies for multiple-level access control by credential category." Scheidt column 2, lines 3-24, which is relied upon to substantiate this position, is such as to set forth:

> According to an exemplary aspect of the invention, a user's profile ("user profile") determines whether and how the user can encrypt (write) and decrypt (access) an object, which can be, for example, a data instance or a computer program. A user profile includes at least one credential, and each credential includes one or both of an asymmetric key pair: a credential public key (write authority) and a credential private key (access authority).

> A user can encrypt (or write) an object with one or more particular credential public keys included in the user's profile, such that subsequent decryption of the encrypted object by another user (or the original user) requires corresponding or otherwise authorized credentials. Accordingly, a user can decrypt an encrypted object if the user possesses, in that user's profile, credentials corresponding to those with which the encrypted object was encrypted. A user can select one or more credentials with which to interact with a particular object or objects in general, or selection of credentials can be automated.

It is submitted that this disclosure would not lead the reader to the conclusions noted above, particularly in light of the fact that the Spies reference does not, for the reasons advanced *supra*, disclose or suggest the use of a credential index. Clearly, there is nothing to suggest an arrangement wherein a list of credential types that one is prepared to disclose, is sent. Neither is there anything to suggest that the recipient selects which credential types are such as to provide an acceptable assurance and that this selection is sent back to the user after which the user reveals the chosen credentials. In other words, there is nothing to suggest the activity which is recited in the claims at least claim 1 or that this is merely another advantage which would flow from the combination of the references in question.

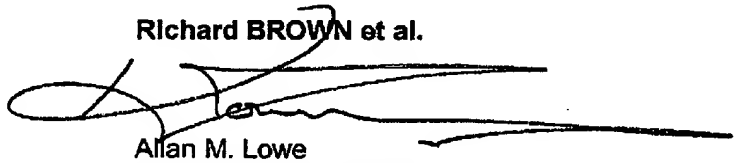
Conclusion

As will be apparent from the preceding remarks, it is clear that the rejection is founded on some clearly unsubstantiated positions with respect to what is disclosed in Spies and may have been inadvertently motivated by a working knowledge of the claimed subject matter when considering the content of the Scheidt et al. reference when considering how to overcome a clearly acknowledged shortcoming of the Spies disclosure. Accordingly, favorable reconsideration and allowance are respectfully requested and deemed in order.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 08-2025, and please credit any excess fees to such deposit account.

Respectfully submitted,

Richard BROWN et al.



Allan M. Lowe
Registration No. 19,641

Keith J. Townsend
Registration No. 40,358

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400
Telephone: 703-684-1111
Facsimile: 970-898-0640

Date: May 1, 2006

AML/dll